IN THE CLAIMS:

Please amend the original claims as follows.

1. (Currently Amended) A method for creating a unique authoritative electronic record, comprising the steps of:

receiving an electronic record into a repository, wherein the repository is contained on an electronic device that stores and executes software;

generating identifying information;

generating a receipt, wherein the receipt includes ~~information relating to~~ a digital signature of a combination of both the electronic record and the appended identifying information;

generating ~~identifying~~ supplemental information that includes a provable representation of the receipt;

prepending the receipt to a beginning of the record;

appending the identifying information and the supplemental information to an ending of the record; and,

storing the record with the prepended receipt and the appended identifying information and supplemental information as the unique authoritative record in the repository.

2. (Currently Amended) The method of claim 1, wherein the step of receiving a record further comprises the step of ~~attaching a time-stamp to~~ time-stamping the electronic record, wherein the time-stamp includes a time and a date when the electronic record was received in the repository ~~and identification information~~.

3. (Currently Amended) The method of claim 1, wherein the receipt comprises at least a digital signature made with a private key of the repository.

4. (Original) The method of claim 1, wherein the repository creates a copy of the authoritative record by copying the record and all information appended to the ending of the record.

5. (Currently Amended) A method for obtaining a digital signature on an authoritative record stored in a secure environment, comprising the steps of:

receiving a request to sign the authoritative record;

computing a ~~partial~~ partially completed message digest of the authoritative record, wherein the partial message digest is related to a proper subset of the authoritative record;

computing a complement of the proper subset;

sending the partial message digest and at least the complement of the proper subset of the authoritative record to a remote location;

~~computing a~~ completing the computation of the message digest, at the remote location, using the partial message digest ~~and~~ , the complement of the proper subset, and identifying information; and,

creating a digital signature with the use of the message digest and a private key.

6. (Original) The method of claim 5, wherein the proper subset of the authoritative record comprises information at a beginning of the authoritative record.

7. (Currently Amended) The method of claim 5, wherein the complement of the proper subset of the authoritative record comprises an electronic record and ending information that is appended at an end of the record.

8. (Currently Amended) The method of claim 5, wherein the step of sending further comprises the steps of sending the partial message digest and the complement of the proper subset of the authoritative record to the remote location in two separate transmissions.

9. (Original) The method of claim 5, wherein software associated with the secure environment is used at the remote location.

10. (Currently Amended) The method of claim 5, further comprising the step of: transmitting at least the digital signature and identifying information to the secure environment.

11. (Currently Amended) A method for creating a unique authoritative record, obtaining and validating a digital signature on the authoritative record, and upon successful validation creating a unique revised authoritative record, comprising the steps of:

receiving a record in a secure environment, wherein the secure environment is connected to a network and comprises at least one server that stores and executes software;

generating identifying information;

generating a receipt, wherein the receipt includes a digital signature of a combination of the record and the appended identifying information ~~relating to the record~~;

generating supplemental ~~identifying~~ information that includes a provable representation of the receipt;

prepending the receipt to a beginning of the record;

appending the identifying information and supplemental information to an ending of the record;

storing the record with prepended receipt and appended identifying information and supplemental information as the unique authoritative record;

receiving a request to sign the authoritative record;

computing a ~~partial~~ partially completed message digest of the authoritative record, wherein the partial message digest is related to a proper subset of the authoritative record;

sending the partial message digest and at least a complement of the proper subset of the authoritative record to a remote location;

~~computing a~~ completing the computation of the message digest, at the remote location, using the partial message digest, ~~and~~ the complement of the proper subset, and other identifying information;

creating a digital signature with the use of the message digest and a private key;

transmitting at least the digital signature and the other identifying information to the secure environment;

validating the digital signature in the secure environment, and upon affirmative validation;

revising the authoritative record with the digital signature and other information to create a revised authoritative record.

12. (Currently Amended) The method of claim 11, wherein the step of receiving a record further comprises time-stamping the record, wherein ~~a time-stamp comprising a time and date the record was received and identification information is attached to the record and the time-stamped record is used as the record in subsequent steps~~ the time-stamp is later attached to the record as part of the identifying information, such that the time-stamp becomes part of the record, wherein the time-stamp comprises a time and date the record was received.

13. (Currently Amended) The method of claim 11, wherein the ~~receipt is a digital signature that~~ digital signature included in the receipt is made with a private key of the secure environment.

14. (Original) The method of claim 11, wherein the proper subset of the authoritative record comprises information at a beginning of the authoritative record.

15. (Currently Amended) The method of claim 11, wherein the complement of the proper subset of the authoritative record comprises the record and ending information that is appended at an end of the record.

16. (Original) The method of claim 11, wherein the step of sending further comprises the steps of sending the partial message digest and the complement of the proper subset of the authoritative record to the remote location in two separate transmissions.

17. (Original) The method of claim 11, wherein software associated with the secure environment is used at the remote location.

18. (Currently Amended) A method for creating and validating at least one digital signature for an electronic authoritative record maintained in a secure environment, wherein control is maintained in the secure environment by software and at least one server, and a copy of the electronic authoritative record can be electronically transmitted to a remote location without losing any of the electronic authoritative record's integrity, the method comprising the steps of:

receiving an electronic record in the secure environment;

generating at least some identifying information;

generating at least some first information comprising a receipt of the electronic record by the secure environment;

defining a beginning information as all information prepended to a beginning of the record and comprising the first information;

generating at least some second information comprising at least a provable representation of the first information, wherein the provable representation of the first information is mathematically related to the first information;

defining an ending information as all information appended to an end of the record and comprising the identifying information and the second information;

creating an authoritative record comprising the beginning information, the electronic record, and the ending information, wherein the beginning information is prepended to the beginning of the electronic record and the ending information is appended to the end of the electronic record;

storing the authoritative record in the secure environment;

making a perceivable copy of the authoritative record by copying only the electronic record and the ending information;

transmitting the perceivable copy of the authoritative record to a remote location;

receiving the perceivable copy at the remote location, and if desired digitally signing the authoritative record by:

generating a ~~partial~~ partially complete message digest ~~of the beginning information,~~ at the secure environment, of the authoritative record, wherein the partial message digest is related to the beginning information;

transmitting the partial message digest from the secure environment to the remote location, completing a message digest of the authoritative record at the remote location with the use of the partial message digest, ~~and~~ the perceivable copy, and other identifying information;

and, creating a digital signature ~~using the message digest~~ at the remote location using the message digest and a private key to produce a digital signature of the authoritative record;

transmitting at least the digital signature and the other identifying information from the remote location to the secure environment;

receiving the digital signature and the other identifying information in the secure environment;

validating the digital signature in the secure environment with the use of the digital signature, a corresponding public key of the private key, and a separately computed message digest of the combination of the authoritative record and the received identifying information in the secure environment, and upon affirmative validation of the digital signature;

generating a revised authoritative record by prepending digital signature information comprising at least the digital signature to a beginning of the authoritative record, wherein the digital signature information is thereby included in the beginning information, appending signature information comprising ~~of~~ at least the received identifying information and a provable representation of the digital signature information to an end of the authoritative record, wherein the ending information thereby includes the signature information;

and, storing the revised authoritative record in the secure environment.

19. (Currently Amended) The method of claim 18, wherein the step of generating a revised authoritative record, further comprises: prepending a signature receipt to the beginning information so that the signature receipt becomes part of the beginning information, wherein the signature receipt comprises at least a unique representation of the revised authoritative record, wherein the unique representation comprises a digital signature; and, appending identifying information and supplemental information to the ending information so that the identifying information and the supplemental information become ~~becomes~~ part of the ending information, wherein the ~~identifying information~~ supplemental information comprises a provable representation of the signature receipt.

20. (Original) The method of claim 18, wherein software associated with the secure environment is stored and used at the remote location.

21. (Original) The method of claim 18, wherein the perceivable copy and the partial message digest are transmitted to the remote location in a same transmission.

22. (Currently Amended) The method of claim 18, further comprising the steps of: sending copies of the revised authoritative record to one or more remote locations by treating the revised authoritative record as the authoritative record and repeating the steps of: making a perceivable copy; transmitting the perceivable copy; receiving the perceivable copy; generating a partial message digest; transmitting the partial message digest; completing a message digest;~~,~~ creating a digital signature; transmitting the digital signature; receiving the digital signature; validating the digital signature; and, generating a revised authoritative record.

23. (Currently Amended) The method of claim ~~19~~ 18, further comprising the steps of: sending copies of the revised authoritative record to one or more remote locations by treating the revised authoritative record as the authoritative record and repeating the steps of: making a perceivable copy; transmitting the perceivable copy; receiving the perceivable copy; generating a partial message digest; transmitting the partial message digest; completing a message digest;~~,~~ creating a digital signature; transmitting the digital signature; receiving the digital signature; validating the digital signature; generating a revised authoritative record; prepending a signature receipt; and, appending identifying information and supplemental information.

24. (Currently Amended) The method of claim 18, wherein the step of receiving an electronic record further comprises: time-stamping the electronic record ~~with a time-stamp that includes a time and date of receipt, and identification information and the time-stamped record is used as the electronic record in the subsequent steps~~ , wherein the time-stamp is later attached to the record as part of the identifying information, such that the time-stamp becomes part of the record, wherein the time-stamp comprises a time and date the record was received.

25. (Currently Amended) The method of claim 18, wherein the ~~first information comprises~~ receipt comprises at least a digital signature made with a private key of the secure environment.

26. (Currently Amended) The method of claim 18, wherein the provable representation of the first information comprises at least a message digest that was used to generate the first information.

27. (Original) The method of claim 18, wherein the step of transmitting the perceivable copy, further comprises: transmitting a cryptographic version of the copy.

28. (Original) The method of claim 18, wherein the partial message digest includes information necessary to continue the creation of the message digest at the remote location.

29. (Currently Amended) The method of claim 18, wherein the step of validating further comprises the steps of: decrypting the digital signature with a public key; and, comparing the decrypted digital signature with a ~~representation of~~ message digest of the combination of the authoritative record stored in the secure environment and the received identifying information.

30. (Currently Amended) A computer readable medium for storing a program that allows a user to receive, and digitally sign a copy of an electronic record that is stored in a remote location, wherein the program provides for the user to:

receive a proper subset of the electronic record, wherein the proper subset of the electronic record allows the user to view, store and print the record, and when the user is ready, to;; sign the electronic record, wherein the program requests and receives at least a partially completed message digest of the electronic record, wherein the partial message digest is related to the complement of the proper subset of the electronic record, and the user then uses the ~~proper subset, the complement of the subset,~~ partial message digest, the proper subset, and identifying information, to complete the computation of the message digest of the electronic record to be signed, and the user then uses the completed message digest and a private key to digitally sign the record.

31. (Currently Amended) The computer readable medium of claim 30, wherein the program provides for transmission of at least the digital signature and the identifying information to the remote location.

32. (Currently Amended) A method for digitally signing an electronic record received from a secure environment, wherein the electronic record consists of a first portion and a second portion, the method comprising the steps of:

receiving the ~~first~~ second portion of the electronic record from the secure environment, wherein the ~~first~~ second portion allows a user to view, print or store the electronic record;

receiving a ~~partial~~ partially complete message digest of the electronic record from the secure environment wherein the partial message digest is related to the ~~second~~ first portion of the electronic record;

~~generating a~~ completing the message digest of the electronic record using the partial message digest, the second portion, and identifying information ~~first portion and the partial message digest~~;

and, creating a digital signature of the electronic record using the message digest and a private key.

33. (Currently Amended) The method of claim 32, further comprising the step of: transmitting at least the digital signature and the identifying information to the secure environment.

34. (Currently Amended) An apparatus for creating and storing a unique authoritative record, comprising: at least one server, connected to a network, that stores and executes software for receiving a record in a secure environment wherein the secure environment is created by the server and the software; wherein the software provides for:

generating identifying information;

generating a receipt, wherein the receipt includes a digital signature of the combination of the authoritative record and the appended identifying information ~~relating to the record~~;

generating ~~identifying~~ supplemental information that includes a provable representation of the receipt;

prepending the receipt to a beginning of the record;

appending the identifying information and the supplemental information to an ending of the record;

and, storing the record with prepended receipt and appended identifying information and supplemental information as the unique authoritative record in the secure environment.

35. (Currently Amended) The apparatus of claim 34, wherein the record is time-stamped, with a time and date the record was received ~~and with identification information~~, immediately after the record is received in the secure environment.

36. (Currently Amended) The apparatus of claim 34, wherein the ~~receipt comprises a~~ digital signature included in the receipt is made with a private key of the secure environment.

37. (Original) The apparatus of claim 34, wherein the secure environment creates a copy of the authoritative record by copying the record and all information appended to the ending of the record.

38. (Currently Amended) ~~An~~ A system for obtaining a digital signature on an authoritative record that is stored in a secure environment, comprising: a server that stores and executes software that creates the secure environment and at least one computer at a remote location that stores and executes at least ~~of~~ a portion of the software, wherein the software provides for:

receiving a request from the remote location to sign the authoritative record;

computing a ~~partial~~ partially completed message digest at the secure environment, of the authoritative record, wherein the partial message digest is related to a proper subset of the authoritative record;

sending the partial message digest and at least a complement of the proper subset of the authoritative record to the remote location;

~~computing a~~ completing the computation of the message digest, at the remote location, using the partial message digest and the complement of the proper subset, and identifying information;

and, creating a digital signature with the use of the message digest and a private key.

39. (Original) The system of claim 38, wherein the proper subset of the authoritative record comprises information at a beginning of the authoritative record.

40. (Currently Amended) The system of claim 38, wherein the complement of the proper subset of the authoritative record comprises a record and ending information that is appended at an end of the record.

41. (Original) The system of claim 38, wherein the partial message digest and the complement of the proper subset of the authoritative record are sent to the remote location in two separate transmissions.

42. (Currently Amended) The system of claim 38, wherein at least the digital signature and the identifying information are ~~is~~ transmitted to the secure environment.

43. (Currently Amended) A system for creating a unique authoritative record, obtaining and validating a digital signature on the authoritative record, and upon successful validation creating a unique revised authoritative record, comprising: at least one server, connected to a network, that stores and executes software that creates a secure environment and at least one computer at a remote location that stores and executes at least ~~of~~ a portion of the software, wherein the software provides for:

receiving a record in the secure environment;

generating identifying information;

generating a receipt, wherein the receipt includes a digital signature of the combination of the authoritative record and the appended identifying information ~~relating to the record~~;

generating ~~identifying~~ supplemental information that includes a provable representation of the receipt;

prepending the receipt to a beginning of the record;

appending the identifying information and the supplemental information to an ending of the record;

storing, in the secure environment, the record with prepended receipt and appended identifying information and supplemental information as the unique authoritative record;

receiving a request, from the remote location, to sign the authoritative record;

computing a ~~partial~~ partially completed message digest, ~~of a proper subset of the authoritative record~~ at the secure environment, of the authoritative record, wherein the partial message digest is related to a proper subset of the authoritative record;

sending the partial message digest and at least a complement of the proper subset of the authoritative record to the remote location;

~~computing a~~ completing the computation of the message digest, at the remote location, using the partial message digest and the complement of the proper subset, and other identifying information;

creating a digital signature with the use of the message digest and a private key;

transmitting at least the digital signature and the other identifying information from the remote location to the secure environment;

validating the digital signature in the secure environment, and upon affirmative validation;

revising the authoritative record with the digital signature and other information to create a revised authoritative record.

44. (Currently Amended) The system of claim 43, wherein the record is time-stamped, immediately after it is received by the secure environment, with a time-stamp comprising a time and date the record was received ~~and identification information~~.

45. (Currently Amended) The system of claim 43, wherein the ~~receipt is a digital signature that~~ digital signature included in the receipt is made with a private key of the secure environment.

46. (Original) The system of claim 43, wherein the proper subset of the authoritative record comprises information at a beginning of the authoritative record.

47. (Currently Amended) The system of claim 43, wherein the complement of the proper subset of the authoritative record comprises the record and ending information that is appended at an end of the record.

48. (Original) The system of claim 43, wherein the partial message digest and the complement of the proper subset of the authoritative record are sent to the remote location in two separate transmissions.

49. (Currently Amended) A system for creating and validating at least one digital signature on an electronic authoritative record that is maintained in a secure environment, wherein a copy of the electronic authoritative record can be electronically transmitted to a remote location without losing any of the electronic authoritative record's integrity, the system comprising: at least one server, connected to a network, that stores and executes software that creates the secure environment and at least one computer at a remote location that stores and executes a portion of the software, wherein the software provides for:

receiving an electronic record in the secure environment;

generating at least some identifying information;

generating at least some first information comprising a receipt of the electronic record by the secure environment;

defining a beginning information as all information prepended to a beginning of the record and comprising the first information;

generating at least some second information comprising at least a provable representation of the first information, wherein the provable representation of the first information is mathematically related to the first information;

defining an ending information as all information appended to an end of the record and comprising the identifying information and the second information;

creating an authoritative record comprising the beginning information, the electronic record, and the ending information, wherein the beginning information is prepended to the beginning of the electronic record and the ending information is appended to the end of the electronic record;

storing the authoritative record in the secure environment;

making a perceivable copy of the authoritative record by copying only the electronic record and the ending information;

transmitting the perceivable copy of the authoritative record to a person at the remote location;

receiving the perceivable copy at the remote location, and if desired digitally signing the authoritative record by:

generating a ~~partial~~ partially completed message digest ~~of the beginning information~~, at the secure environment, of the authoritative record, wherein the partial message digest is related to the beginning information;

transmitting the partial message digest from the secure environment to the remote location, completing a message digest of the authoritative record at the remote location with the use of the partial message digest, ~~and~~ the perceivable copy, and other identifying information;

and, creating a digital signature at the remote location using the message digest ~~at the remote location~~ and a private key to produce the digital signature of the authoritative record;

transmitting at least the digital signature and the other identifying information from the remote location to the secure environment;

receiving the digital signature and the other identifying information in the secure environment;

validating the digital signature in the secure environment with the use of the digital signature, a corresponding public key of the private key, and a separately computed message digest of the combination of the authoritative record and the received identifying information in the secure environment, and upon affirmative validation of the digital signature;

generating a revised authoritative record by prepending digital signature information comprising at least the digital signature to a beginning of the authoritative record, wherein the digital signature information is thereby included in the beginning information, appending signature information comprising ~~of~~ at least the received identifying information and a provable representation of the digital signature information to an end of the authoritative record, wherein the ending information thereby includes the signature information;

and, storing the revised authoritative record in the secure environment.

50. (Currently Amended) The system of claim 49, wherein generating a revised authoritative record, further comprises: prepending a signature receipt to the beginning information so that the signature receipt becomes part of the beginning information, wherein the signature receipt comprises at least a unique representation of the revised authoritative record, wherein the unique representation comprises a digital signature; and, appending

identifying information and supplemental information to the ending information so that the identifying information and supplemental information become ~~becomes~~ part of the ending information, wherein the supplemental ~~identifying~~ information comprises ~~of~~ a provable representation of the signature receipt.

51. (Original) The system of claim 49, wherein the perceivable copy and the partial message digest are transmitted to the remote location in a same transmission.

52. (Currently Amended) The system of claim 49, wherein the software further provides for sending copies of the revised authoritative record to one or more remote locations by treating the revised authoritative record as the authoritative record and repeating the steps of: making a perceivable copy; transmitting the perceivable copy; receiving the perceivable copy; generating a partial message digest; transmitting the partial message digest; completing a message digest~~,~~; creating a digital signature; transmitting the digital signature; receiving the digital signature; validating the digital signature; and, generating a revised authoritative record.

53. (Currently Amended) The system of claim ~~50~~ 49, wherein the software further provides for sending copies of the revised authoritative record to one or more remote locations by treating the revised authoritative record as the authoritative record and repeating the steps of: making a perceivable copy; transmitting the perceivable copy; receiving the perceivable copy; generating a partial message digest; transmitting the partial message digest; completing a message digest~~,~~; creating a digital signature; transmitting the digital signature; receiving the digital signature; validating the digital signature; generating a revised authoritative record; prepending a signature receipt; and, appending identifying information and supplemental information.

54. (Currently Amended) The system of claim 49, wherein the electronic record is time-stamped immediately after being received in the secure environment, and the time-stamp comprises a time and date of receipt~~, and identification information~~.

55. (Currently Amended) The system of claim 49, wherein the receipt ~~first information~~ comprises at least a digital signature made with a private key of the secure environment.

56. (Currently Amended) The system of claim 49, wherein the provable representation of the first information comprises at least a message digest that was used to generate the first information.

57. (Original) The system of claim 49, wherein a cryptographic version of the perceivable copy is transmitted to the remote location.

58. (Original) The system of claim 49, wherein the partial message digest includes information necessary to continue the creation of the message digest at the remote location.

59. (Currently Amended) The system of claim 49, wherein validation further comprises: decrypting the digital signature with a public key; and, comparing the decrypted digital signature with a ~~representation~~ message digest of the combination of the authoritative record stored in the secure environment and the received identifying information.

60. (Currently Amended) An apparatus for digitally signing an electronic record that is received from a secure environment, wherein the electronic record consists of a first portion and a second portion, comprising: a computer that stores and executes software, wherein the software provides for:

receiving the ~~first~~ second portion of the electronic record from the secure environment, wherein the ~~first~~ second portion allows a user to view, print or store the electronic record;

receiving a ~~partial~~ partially completed message digest ~~of the second portion~~ of the electronic record from the secure environment, wherein the partial message digest is related to the first portion of the electronic record;

~~generating a~~ completing the message digest of the electronic record using the partial message digest, the second portion, and identifying information ~~first portion and the partial message digest~~;

and, creating a digital signature of the electronic record using the message digest and a private key.

61. (Currently Amended) The apparatus of claim 60, wherein the computer transmits at least the digital signature and the identifying information to the secure environment.

62. (New) The method of claim 18, wherein the step of validating further comprises the step of: using the digital signature; a public key; and a message digest of the combination of the authoritative record stored in the secure environment and the received identifying information; along with a validation algorithm; to validate the signature.

63. (New) The system of claim 49, wherein validation further comprises: using the digital signature; a public key; and a message digest of the combination of the authoritative record stored in the secure environment and the received identifying information; along with a validation algorithm; to validate the signature.

64. (New) A method for creating a unique authoritative electronic record, comprising the steps of:

receiving an electronic record into a repository, wherein the repository is contained on an electronic device that stores and executes software;

generating a receipt, wherein the receipt includes a digital signature of the electronic record;

generating supplemental information that includes a provable representation of the receipt;

prepending the receipt to a beginning of the record;

appending the supplemental information to an ending of the record; and,

storing the record with the prepended receipt and the appended supplemental information as the unique authoritative record in the repository.

65. (New) A method for obtaining a digital signature on an authoritative record stored in a secure environment, comprising the steps of:

receiving a request to sign the authoritative record;

computing a partially completed message digest of the authoritative record, wherein the partial message digest is related to a proper subset of the authoritative record;

computing a complement of the proper subset;

sending the partial message digest and at least the complement of the proper subset of the authoritative record to a remote location;

completing the computation of the message digest, at the remote location, using the partial message digest and the complement of the proper subset; and,

creating a digital signature with the use of the message digest and a private key.